ABSTRACT OF THE DISCLOSURE

MANAGING AND EXTENDING ATTRIBUTE VALUES FOR PUBLIC KEY CRYPTOGRAPHY STANDARDS

A method and system for processing PKCS-attributes in heterogeneous environment and user-defined attributes is provided. Attributes are registered with a PKCS9 gateway class, and the attributes include user-defined attributes and PKCS-standard defined attributes. Each of the registered attributes is associatively stored with an identifier. A method in the PKCS9 gateway class may be called with a parameter containing an object identifier for an attribute. An attribute mapping data structure is searched using the object identifier in the received parameter, and in response to finding a matching object identifier, a class identifier that has been associatively stored with the matching object identifier is retrieved from the attribute mapping data structure. A method in the class identified by the class identifier is then called. The called method may include an operation for construction, attribute conversion to and from DER-encoding, attribute differentiation, and attribute value extraction. A class hierarchy of attribute types is based on an abstract class for all attribute objects with a subclass for undefined attributes and a subclass for defined attributes. The subclass for defined attributes is further decomposed into a subclass for each PKCS-defined attribute and a subclass for each user-defined attribute.